REMARKS

We have amended claims 55, 60, and 76 to address the informalities identified by the examiner and we have amended claim 54 to address the examiner's 35 U.S.C. §112, second paragraph, concerns.

The examiner rejected claims 54-69, 3-4, 10, and 70-90 under 35 U.S.C. §112, first paragraph, on the basis that they supposedly contain subject matter that was not described in the specification. More specifically, the examiner objected to the use of the term "encrypted container." We note, however, that the specification does in fact support the use of this term. The specification states that "the term 'personal security device' refers to encrypted sensitive information" (p. 8 lines 28-29). In other words, the specification describes an encrypted device. It also mentions "decrypt[ing] the personal security device (Step 195) thereby gaining access to its contents" (p. 12 lines 4-5). That is, the device has contents, and therefore by definition it is a "container." Moreover, its contents are encrypted. Thus, we submit that a person of skill in the art would readily understand the meaning of encrypted container especially in view of the description found in the specification.

The examiner rejected claims 1, 11, 52, and 53 under 35 U.S.C. §103(a) as being unpatentable over Holloway (U.S. 6,424,718) in view of Linehan (U.S. 5,495,533). The examiner now admits that Holloway fails to teach:

> (c) at an authentication server, receiving authentication information from the client; and
> (d) responsive to said authentication information, sending from a key server to the client decryption information for said personal security device.

To supply that which is missing, the examiner relies on Linehan who supposedly teaches these elements. The examiner argues that it would be obvious to incorporate them into Holloway for the following reasons:

> ...because disadvantages of manual key management (such as entering Holloway's owner's pass phrase PPu) include the awkward and time-consuming requirements for end-users to enter encryption keys, the possibility that users may forget keys, the inability to access encrypted files when the individual who knows the keys is unavailable.

However, we submit that the reasons identified by the examiner would not motivate a person of ordinary skill in the art to modify Holloway in the manner proposed by the examiner. For one thing, Linehan does not eliminate the need for the user to remember and enter passwords; so, the changes proposed by the examiner do not address that problem. For another, Linehan addresses the problems of forgetting passwords, not by storing passwords on another server, but rather by storing the key in an unencrypted form so that the unencrypted key can be accessed by anybody with access to the key server.

Including the personal key server and authentication server of Linehan in the system of Holloway would not address the "disadvantages of manual key management," as argued by the examiner. As pointed out by the examiner, the Holloway system requires that the user remember the pass phrase PPu. But that is true of the Linehan system, which also requires the user to enter his identity and a pass phrase. Linehan discloses that "[t]he 'foundation' for access to files is the Kerberos or KryptoKnight authentication of individual users" (col. 11, lines 7-9). According to Linehan, a user authenticates to Kerberos by also using a userid and a password:

> Typically, users identify themselves by executing a login process that involves entering a computer userid and matching password. The mechanism [f]or validating the userid and password, and for maintaining the connection between the user and any processes run on behalf of the user, is called user authentication (col. 2 lines 63-67 and col. 3 line 1).
>
> A network authentication mechanism, such as Kerberos (reference 8), keeps the password file on a authentication server 20 as shown in FIG. 3. A special protocol is used to validate a userid and password entered on a user computer 22 against the password file on the authentication server 20. (col. 3 lines 10-14).

Thus, the modifications proposed by the examiner would simply add a layer of complexity to the Holloway system without reducing the burden placed on the user. So, a person skilled in the art would not be motivated on the basis of reducing burden to modify the Holloway system to include the personal key server and authentication server of Linehan.

As recognized by the examiner, Linehan's system is also designed to enable somebody to access the key if the user is not available or has forgotten his or her password. But Linehan does this by storing the key in an unencrypted form on the key server, not by providing another server for storing the user's password. Linehan addresses the security risks associated with sending an unencrypted key to a client by using session keys to encrypt the transmissions:

> The messages sent between the Personal Key Client and the Personal Key Server are themselves encrypted in session keys that are provided by Kerberos. This "double encryption" ensures that the file encryption keys themselves do not appear in the clear on the communication path between the Client and the Server. (Col. 8, lines 18-23).

Thus, if a person skilled in the art were motivated to modify Holloway's system to address the problem of the forgotten password, that person would store the key SKu in unencrypted form on key server 138 and then use session keys to transmit that key to the user. But modifying the Holloway system in that way does not produce the claimed invention.

For at least the reasons above, claims 1 and 11 are not obvious over Holloway in view of Linehan. For similar reasons, claims 54 and 70 are also not obvious over Holloway in view of Linehan. In view of the above amendment, applicants believe the pending application is in condition for allowance.

Dated:

Respectfully submitted,

By____________________
Eric L. Prahl
Registration No.: 32,590
WILMER CUTLER PICKERING HALE AND DORR LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000
Attorney for Applicant